# 具電腦鑑識特性之即時遠端 log 蒐集監測機制

古東明　陳弘傑　沈志昌
雲林科技大學資訊管理所
koo@yuntech.edu.tw　g9323717@yuntech.edu.tw　g9220804@yuntech.edu.tw

## 摘要

電腦鑑識科學為用來判定電子犯罪常使用的利器，然而，卻有著缺乏資料及可靠度不足時，就無法有效使用的缺憾。而電腦鑑識的數位證據必須具備兩種要件才可接受，一為所蒐集的證據必須是原始的，無人為介入產生或偽造的可能；二為分析前後的數位證據與原始證據前後一致。本研究即是基於電腦鑑識之前提下提供一個可靠的遠端 log 即時監測蒐集機制，可提高所蒐集之 log 資訊的可靠度及代表性，提供後續電腦鑑識分析上原始資料的可靠度，做到資料即可代表原始環境之特性，提供法院作為呈堂證據，透過 SOC 之架構，可以達成蒐集廣範圍之 log 資訊，簡易整合在企業組織之 SOC 架構，建構一個完整的企業安全防範體制，確保企業資訊安全。

**關鍵詞**：電腦鑑識、SOC、Log、數位證據。

## 1. 前言

現今生活受網際網路的影響甚鉅，其無遠弗屆的特性以及跨越了時間與空間上的限制，使得人們可以藉由網際網路從事各式各樣的活動，雖然網際網路讓我們的生活更便利，但如果被一些意圖不軌的犯罪者利用其特性，找尋漏洞且伺機攻擊，將會造成莫大的損失。近年來，網路攻擊事件頻傳，各國政府以及企業也已經開始正視這個問題，紛紛制訂相關法令以及採取網路安全的防護措施，目的就是要遏阻這些犯罪者，減少資安事件的發生。

目前這些網路安全的防護措施或系統，隨著犯罪手法的不斷翻新也持續地在改進，這儼然已經變成了彼此雙方的攻防角力戰，防守一方稍一疏忽，可能就會造成無法挽回的後果。防護系統需能夠有效地蒐集及監測這些網路資訊，若有異常發生時，能夠即時地回報警訊並且採取相對應的應變措施。但要防堵所有的攻擊做到滴水不漏，其實是非常困難的。也因此電腦鑑識學（Computer Forensics or Cyber Forensics）也因運而生。

電腦鑑識學是近年來新興的一項研究領域，目的在於從電子媒體尋找入侵攻擊之證據，作為法律定罪上的證據，其分為現場蒐證及實驗室分析兩步驟，因此，所蒐集到之資訊，必須要絕對可以代表犯罪方之行為，否則所蒐集之證物將功虧一簣，然而，電子資訊有著容易攜帶及修改之特性，因此如何有效取得最具代表性之資料，則是此一領域裡蒐集資料的重點之一。雖有電腦鑑識科學輔助，從歷史資料及各案例中卻突顯出一個事實，即是使用者端的歷史資料早已遭受破壞，甚至是沒有完整設定，造成所能使用的資訊過少，無法進行分析，喪失定罪的最佳證據，這都是在鑑識上所遭遇的困難。

主機維護一直是系統管理者日常最重要之例行事務，然而，系統管理的複雜度、效率和所管理範圍、主機數、主機型態息息相關，然而，主機為一封閉之系統，有許多案例指出，系統發生錯誤，甚至嚴重影響到組織之運作，卻無法有效查出問題發生之癥結，或是判讀事件發生來源，最大的原因在於沒有紀錄。

因此，事件記錄檔(LOGs)的概念被廣泛使用在系統管理上，透過事件記錄檔機制，主機系統運作之軌跡能夠被有效的記錄，也讓系統管理者能夠循跡找出問題癥結，對於系統管理者而言，log檔案的存在性是絕對必要。

SOC(security operation center)架構提供了整體

監控的特性，然而，SOC 著重在於及時發現問題、處理問題，對於遭受入侵後的後續處理仍有所不足之處，因此，本研究目的在於結合 SOC 之架構，建立可搭配電腦鑑識特性之遠端及時 log 蒐集監測系統。

透過此遠端及時 log 蒐證系統，將可以確保遠端及時 log 資料蒐集時的可靠度，以及達到所記錄之資料可以充分代表原始資料，藉此提升在電腦鑑識上之可用度，提供發生資安事件後尋找犯罪證據及分析最好背書。

SOC 架構及電腦鑑識作業，在資訊安全應用上皆是相當具有貢獻的發展，也逐漸被資訊安全管理議題所重視，本研究將焦點放置於結合兩種架構之優點，提供經費及設備不足之中小型組織建立一具有電腦鑑識特性之遠端 log 監測機制，亦可稱為具電腦鑑識特性下之 Light-SOC 架構，透過此方式來達到監測管理範圍下之系統及網路節點，並且若不幸發生資安事件，除可即時預警外，所記錄之資料亦可以較具有效率，且兼顧可用性之資料提供給予分析單位進行後續鑑識判斷工作，大幅降低鑑識作業處理上所帶來的影響。

## 2. 文獻探討

### 2.1 電腦鑑識技術

電腦鑑識技術（Computer forensics or Cyber forensics）在犯罪鑑識上被視為一項重要的環節，目的在於取得數位電子證據，提供偵辦電子犯罪上的參考及法庭證據，因此必須著重證物的可用性（useful）及唯一性（individual），如此才能在整個鑑識程序上被承認該證物是可以完全代表原始環境[4]。而其方法與基本原則為[3]：

（1）在不改變或破壞證物的情況下取得原始證物。

（2）證明所抽取的證物來自扣押的證物。

（3）在不改變證物的情況下進行分析。

### 2.2 使用金鑰的單向雜湊函數

使用金鑰的單向雜湊函數又稱為訊息鑑別碼（Message Authentication Code，MAC）[2]。MAC 和一般的單向雜湊函數有許多相同的特性，但是卻多了一項鑑別金鑰的機制；換句話說，只有擁有鑑別金鑰的人才人對MAC進行核驗。而這種植基於密碼理論雜湊函數的MAC即稱作HMAC。

MAC通常用於不同使用者間的訊息核驗，或是用來檢視文件是否遭到修改。在檢視文件是否遭到竄改時，使用者可對文件進行MAC計算，並儲存MAC的輸出值。當文件遭竄改時，可經由從新計算MAC，並比對新舊MAC的不同來發覺。在這個情況，如只使用一般單向雜湊函數，則竄改者可自行計算一個新的雜湊函數值，來取代原先的雜湊函數值，此時文件所有人就無法經由雜湊函數值之比對來發現文件曾遭竄改。而在採用HMAC的情況下，除非鑑別金鑰遭到瓦解，否則任何非經授權者皆無法製作出正確的HMAC值。

一個簡單的 HMAC 可由一般的單向雜湊函數加上非對稱金鑰系統的加密實做完成；目前已知的 HMAC 系統也多採用此一類似的方式。

### 2.3 數位證據

所謂「數位證據」（Digital Evidence）泛指任何在網路犯罪過程中，利用電腦或是網路所產生亦能被儲存、傳輸或取得之具犯罪事實認定效力的二位元（binary）型態資料。此外，數位證據具有不易取得、易複製、易消滅、易竄改的特性，想要在資訊安全事件發生後取得相關的數位證據，則必須要有一完善的收集、擷取、分析及保存數位證據的方法[1]。通常企業會藉由內部網路設備或防護性軟硬體設施如 網路伺服器（network server）、代理伺服器（proxy server）、防火牆（firewall）或入侵偵測系統（intrusion detection system）等來進行連線控管與稽核的動作。而最常見的稽核方式即是將有意義的系統或網路事件，以各種形式的歷史稽核檔（log 檔）儲存在企業所指定的儲存媒介上，作為網路管理者查核的依據。這些平時收集到的紀錄亦可做為輔助認定網路犯罪的數位證據。

## 2.4 事件記錄分析機制

主機維護一直是系統管理者日常最重要之例行事務，然而，系統管理的複雜度、效率和所管理範圍、主機數、主機型態息息相關，然而，主機為一封閉之系統，有許多案例指出，系統發生錯誤，甚至嚴重影響到組織之運作，卻無法有效查出問題發生之癥結，或是判讀事件發生來源，最大的原因在於沒有紀錄。

因此，事件記錄檔(LOGs)的概念被廣泛使用在系統管理上，透過事件記錄檔機制，主機系統運作之軌跡能夠被有效的紀錄，也讓系統管理者能夠循跡找出問題癥結，對於系統管理者而言，log 檔案的存在性是絕對必要。

在資訊安全意識抬頭之今日，log 檔對於系統更突顯出其存在之必要，然而，對於系統管理者，log 檔的存在其實是個相當矛盾的問題，事件記錄檔能夠有效的儲存系統所有執行步驟，可以進一步還原。然而，log 最令人詬病之問題在於如何有效的儲存，在企業組織內，資訊保存政策除了保存重要檔案外、系統記錄檔的保存也是開始被重視的一環，從 BS7799 規範中可窺得一斑。

商業型態著重於網路服務及主機服務之供應商，對於系統記錄檔的重視更是其來有至，尤其在網路安全事件頻繁之現今，事件記錄檔的存在更是日益重要，尤其在進行入侵分析時，事件記錄檔的存在，往往決定了事件還原與蒐證的關鍵，妥善的保存事件記錄檔儼然成了資訊安全的重要項目。

### 2.4.1 log 分析遭遇問題

事件記錄檔的存在能夠提供系統管理者一個參考並且回溯事發環境的工具，然而，對於系統管理者來說，log分析是相當龐大的負擔，原因如下：

- 事件記錄檔種類過多
- 事件記錄檔內容過於龐大
- 事件記錄檔只反應當時狀態
- 事件記錄檔保存不易

由於事件記錄檔只忠實反應該時間點系統狀態，因此，對於任何步驟都將忠實地紀錄下來，會導致系統記錄檔過於龐大，且記錄檔中之訊息複雜度並非以系統是否有錯誤而決定，而是以系統所能記錄的種類多寡來記錄，因此會導致該時間點也許是正常狀況、但是到了某個時間點卻是異常狀況，讓系統管理者不敢貿然進行檔案之刪除，在刪與不刪間取捨也是系統管理者煩惱之一。再者，在發生異常事件之判讀上，log 檔雖有著紀錄系統狀況之功能，但是否能有效或是快速尋找出問題之癥結，並非是每一個系統管理員能夠勝任，尤其隨著應用系統數量的多寡，也造成系統管理員在「茫茫 log 海」裡要尋找出問題癥結，有時會因為 log 檔案過於龐大，宛若大海撈針般之困難，讓許多系統管理員感受許多壓力[6]。因此有效的過濾事件記錄檔並且尋求更有效率的呈現事件記錄檔內容成為事件分析機制是否成功的關鍵因素。

## 2.5 Security Operation Center (SOC)

安全作業中心（Security Operation Center, SOC）是一整合性的安全監控機制，目的在於管理大範圍且不同平台主機，負責監控並且針對安全入侵事件做出應對的管理機制，相同概念的架構有 NOC（Network Operation Center）兩者最大不同在於所檢測之對象，SOC 目的在於網域下的主機安全事件，而 NOC 則是針對網路節點進行流量及異常狀況的監控，一個完整的 SOC 會包含五個子系統，分別為 event generations、collection system、formatted messages database、analysis system 及 reaction system，透過五個系統的合作，可以達到中央監控的作用，隨時監控受測主機並在遭遇安全事件時做出正確反應[5]。

SOC 架構有助於幫助系統管理員管理大範圍主機安全性問題，對於分散且不同平台主機，SOC 提供了整合性的概念且透過集中式管理，可以增加管理上的效率，減少時間及空間上的損耗，當然，對於事件資料的蒐集的傳輸安全性是 SOC 在設計時的重點之一，SOC 有助於處理企業組織複雜網路

環境或是主機分散多處的管理問題，透過 SOC 概念，可解決安全檢測與管理議題上的衝突，達到安全管理目的。

SOC 固然可以提供一個完整的安全監控機制，但是由於 SOC 架構過於龐大，需將企業內的系統都納入整個 SOC 架構裡，而為了因應系統的複雜性，需要量身訂做 SOC，也因此需要耗費大量的金錢在購買軟、硬體以及人才的培訓上面，因此 Light-SOC 的建立是有其必要性的。

## 3. 研究方法

本研究將以 Web-Based 做為開發系統之基礎，以 Linux 做為系統工作之平台，建立具電腦鑑識特性之即時遠端 log 監測蒐集機制，管理者可以透過 web 方式進行系統管理與監測，而在電腦鑑識基礎下的建構方式，將可提供資料傳輸可靠度，及後續資料可用度之功效，後續面臨電腦鑑識作業時，將可加速鑑識蒐集程序，除對檢調方可以節省時間外，對於受影響之主機，亦可加速復原之時效，降低因為蒐證時需停機的困擾，而正常情況下，Light-SOC 系統亦將持續監控且可透過自行設定之多種預警通知方式來通知管理者，達到即時復原處理之目的，也因此，本研究將重點放置具電腦鑑識特性之 Light-SOC 架構，目的在於結合兩種架構之優勢，減少管理者建置上的浪費，提升系統的可用度。

### 3.1 即時 Log 蒐集機制

資料同步所使用之方法有相當多種，如在異地備援時常使用的 rsync 套件，透過同步的方式可以取得遠地端主機的資料，防止資料遺漏，然而，log 的特性在於隨時都會產生報告在原始 log 檔案（以 linux 為例，會產生於/var/log/message），因此，傳統使用定期同步傳輸的方式將不適用於本架構內，所幸 syslogd 提供了遠端同步模式可提供使用者利用遠端記錄模式來進行資料的蒐集，透過語法的設定，可以達成以一部蒐集主機即時記錄多部監控主機 log 資料之功能。

Log 遠端蒐集機制所使用之通訊協定為 UDP 方式傳輸，UDP 方式並不確保資料的可靠性。而在電腦鑑識的認定下，資料的短少，就可能造成在判決上遭受駁回的疑慮，因此，如何有效做到即時同步且確保每筆資料皆可正確被接收端所接收，則是本研究的重點所在。

我們預計設計使用 syslog-ng 取代原有的 syslog，syslog-ng 使得利用 syslog protocol 進行遠端紀錄傳送時可以確認傳輸的方式或以 TCP 進行，取代原有的 syslog 使用 UDP 傳送等問題。

### 3.2 Light SOC 架構

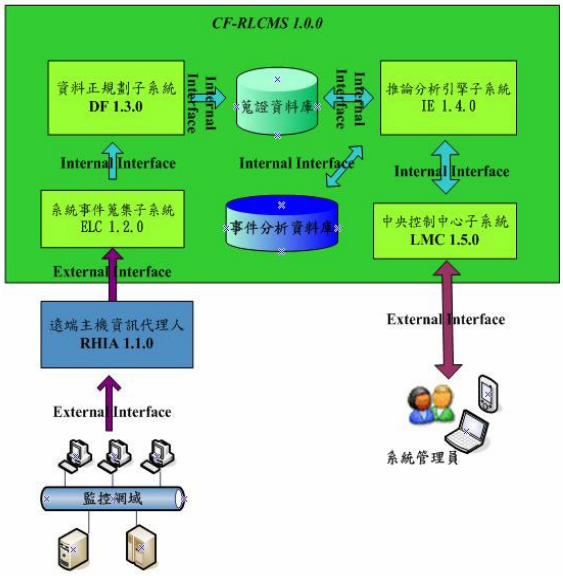


**圖 1 Light SOC 架構圖**

SOC（安全作業中心，或是網路作業中心）最大的目的在於建立大範圍的網路節點監控中心，其最大之目的在於廣泛蒐集來自受管理範圍內所有監測點所提供的資訊，其中資訊包含了封包資訊、檢測主機之主機狀態，完整的安全中心必須兼顧上述各問題，然而，對於經費有限之企業組織，並未能建立如此完善之監測架構，若將目標設置於網路設備之 log 資料、監測主機之服務 log 資料，其實已經可以做到錯誤發生時立即預警、通知管理員修復的目的，因此，本研究預計建立一 Light-SOC 架構提供管理員可以自行安裝，設置監測節點的方式來建立一簡易且具有效率之安全作業中心，如圖 1。

### 3.2.1 遠端主機資訊代理人

遠端主機資訊代理人與即時Log蒐集機制為相結合之系統，主要提供使用者在遠端建立蒐集機制，受網域控管之主機必須在本機中設定此一代理人，透過代理人將會提供可靠性傳輸方式，並且即時將受監測主機產生的 Log 資訊記錄至中央主機中，進行下一個步驟，因此遠端主機資訊代理人作為本架構中最先前的子系統，透過該子系統將能提供所掌控範圍內的所需資訊。

### 3.2.2 系統事件蒐集子系統

本子系統主要目的為提供管理員設定來自遠端主機資訊代理人所傳遞的 Log 資訊，透過代理人概念，RHIA 會將原始 Log 轉化為具有 Hash 的識別碼，以及透過 TCP 通道來完成傳送工作。因此，經由遠端資訊代理人所傳遞的 Log 資訊將會由本子系統所接收。

### 3.2.3 資料正規劃子系統

資料正規劃子系統，主要提供 Log 資料切割存放功能，經由遠端蒐集資料除了型態複雜外，其內部敘述也不同，如何能夠有效的進行區別與存放，將會影響後續進行異常狀態判斷與推論之成效，因此，本子系統目的在於利用正規劃與設計好之切割法則進行 Log 敘述句的切割，並且在切割後存入結論資料庫中，等待推論分析引擎子系統進行處理。本子系統利用兩個資料庫來存放資料，蒐證資料庫用來存放完整蒐集 Log 以及其 hash 值，此資料庫一經存放後即不再進行更動，可以選擇的是利用第二存放設備來存放此資料，此種設計方式目的在於提供後續進行電腦鑑識程序時，可以擁有監控主機完整資訊，可以解決傳統電腦鑑識程序無法完整蒐集受害主機證據的窘境，搭配 hash 值將可進一步驗證該資料的唯一性

### 3.2.4 推論分析引擎子系統

推論分析引擎子系統，本子系統主要提供系統推論異常狀態使用，Log 資訊會反應出目前監測主機操作狀態，過多的 Log 資訊使用者卻無法一一觀察並且進行除錯，利用正向推論方式過濾出有問題的 Log 訊息，並利用反向推論方式減少假警報的產生。困擾系統管理者，被判訂定假警報者會直接不予理會，而真正的錯誤狀態，會被丟入推論結果資料庫中，留待中央控制中心進行預警狀態輸出。

### 3.2.5 中央控制中心

中央控制中心為 web-base 管理機制，整體設計概念承襲 SOC 之架構，透過中央進行主機之監控，可以解決時間及空間上管理之問題，也提供系統管理員一個整合式管理機制，提供事件處理效率，在中央控制中心分為四個子功能分別為：

- 即時監控：即時監控系統內 log 狀態，透過搜尋 log 資訊的方式，也可以達到尋找 log 內可疑事件的目的，可以早先發覺事件的發生，儘早預防。
- 安全風險分析：圖表方式表達受監測主機目前風險程度，圖形化介面可以表達大量資訊之目的，也能讓管理者瞭解風險指數，判斷處理之時機。
- 系統狀態：各受測主機之詳細狀態、包括警示、受攻擊資訊、目前狀態等，可針對各主機進行更詳細資訊判讀。
- 層級式預警：除即時監控系統資訊，事件通知也是監控中心設計上的一項重點，透過預警通報可以通知管理者儘早發現問題之所在，達到快速解決問題，因此，此一功能上除了可以郵件通知管理者事件外，亦設計可由管理者自行設定預警通知的等級，彈性設計可讓管理者自行決定，減少不必要的資訊。

## 3.3 加入 HMAC 機制

HMAC 通常用於不同使用者間的訊息核驗，或是用來檢視文件是否遭到修改。如果能夠有效地管理使用的 key，則 HMAC 亦可用以作為身分驗證使用，請參文後附圖 2。

(1) 當 syslog-ng 收到主機所傳送出來的 log 資料時，在 log messages 前端加上該主機所擁有的 secret key（K），送到 Hash function 中，產出 Digest 值，將原始的 log messages 與其依附的 Digest 值存入資料庫中並且透過 TCP 將這些資料傳送到遠端中央 collection server。

(2) 將收到的 log messages 加上(D)儲存於 collection server 裡所規劃好的資料庫中。每一台在 SOC 所監控範圍的主機都有其 secret key（K），並由 SOC 管理者保存之，以作為日後發生資安事件時，可供 log messages 驗證之用，由於每一主機或伺服器有獨立的(K)，故可以進行驗證訊息為哪一主機或伺服器所發出。又經由配合(K)加上儲存於 collection Server 中的 log messages 可以驗證訊息是否經竄改或改變，對照原本儲存於主機或伺服器中的資訊可作為第二重的確認訊息是否經竄改或改變。

(3) 在 collection server 中，已將欲監測的主機或伺服器所產生的 log messages 儲存至資料庫中，接下來的工作即是利用 SOC 定義的分析機制、規則等來過濾與呈現事件或訊息，供 SOC 人員進行即時監測工作。

## 4. 結論

本研究提供了經費及設備不足之中小型組織建立一具有電腦鑑識基礎之遠端 log 監測機制，透過此方式來達到監測管理範圍下之系統及網路節點，並且若不幸發生資安事件，所記錄之資料可以較具有效率，且兼顧可用性之資料提供給予分析單位進行後續鑑識判斷工作，大幅降低鑑識作業處理上所帶來的影響。

## 參考文獻


[1] 鄭進興，林敬皇，沈志昌，林宜隆，電腦鑑識方法與程序之研究，TANET 2003 研討會論文集，2003，ID 9961。

[2] 單向雜湊函數，http://dsns.csie.nctu.edu.tw/course/intro-secutity/2005/book/chap06.pdf.

[3] G. Kruse II and J. G. Heiser, Computer Forensic: Incident Response Essentials, Addison Wesley, 2002, pp:2-8,163-174.

[4] Kruse, W. & Heiser, J. (2002). Computer forensics：Incident response essentials. Boston：Addison Wesley.

[5] Renaud Bidou, “Security Operation Center Concepts & Implementation”

[6] Stefan Axelsson, Ulf Lindqvist, Ulf Gustafson, Erland Jonsson, ”An Approach to UNIX Security Logging” Proc. 21st National Information Systems Security Conference,1998, pp 62-75.


## 致謝


本計畫承蒙國科會自由軟體專案計畫補助
計畫編號：NSC 94-2218-E-224-007
承蒙國科會計畫 TWISC@NCKU 專案計畫補助
計畫編號：NSC 94-3114-P-006-001-Y


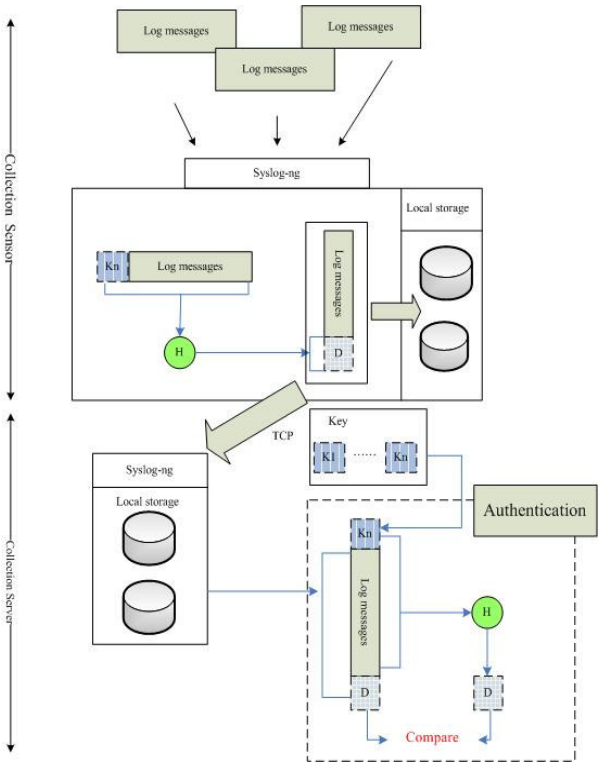


圖 2 本系統與 HMAC 機制